(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－126009
（P2001－126009A）
(43)公開日　平成13年５月11日(2001.5.11)

(51)Int.Cl.'		識別記号	Ｆ Ｉ		テーマコード'(参考)	
Ｇ０６Ｆ	19/00		Ｇ０９Ｃ	1/00	６６０Ｃ	５Ｂ０４９
	17/60		Ｇ０６Ｆ	15/30	Ｌ	５Ｂ０５５
	17/30			15/21	３４０Ａ	５Ｂ０７５
Ｇ０９Ｃ	1/00	６６０		15/30	Ｍ	５Ｊ１０４
					３４０	

審査請求　未請求　請求項の数13　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－310090

(22)出願日　平成11年10月29日(1999.10.29)

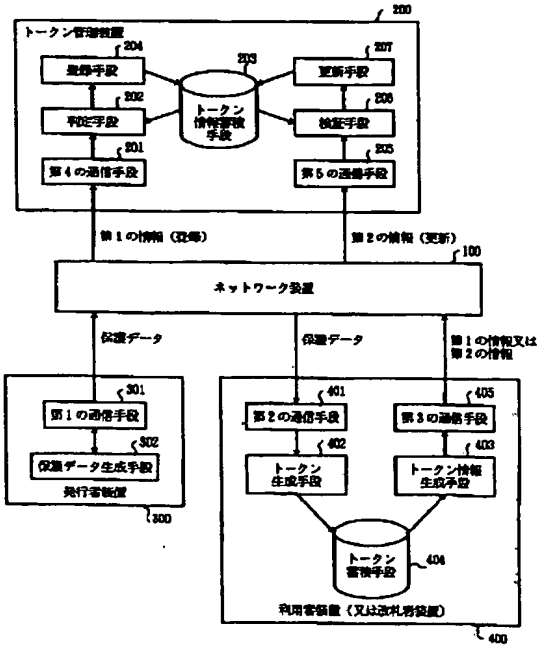
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　藤村　考
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　松山　一雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法

(57)【要約】　（修正有）
【課題】　保護データの所有者を効率的に認証でき、誰でも利用できる汎用的な電子情報流通方法及びシステムを提供する。
【解決手段】　多重使用を防止すべき保護データを生成し、送信する発行者装置と、保護データを受信し、保護データの所有者を特定する情報であるトークンと、トークンを特定するトークン情報を生成して、蓄積し、保護データを特定する保護データＩＤとトークン情報を含む第１の情報を送信する利用者装置と、第１の情報を受信し、保護データＩＤと等しい値を持つ第１の情報が既に蓄積されているかを判定し、蓄積されていない時のみ第１の情報を蓄積し、既に蓄積されている第１の情報を特定する保護データＩＤと更新後のトークン情報とを含む第２の情報を受信し、第２の情報の送信元の装置が第１の情報に含まれるトークン情報によって特定される保護データを保有している時のみ第１の情報を更新するトークン管理装置とを有する。

本発明の原理構成図



【特許請求の範囲】
【請求項１】　電子的な情報の流通を行う情報流通システムであって、
電子情報であり、多重使用を防止すべき保護データを生成する保護データ生成手段と、
前記保護データを送信する第１の通信手段とを有する発行者装置と、
前記保護データを受信する第２の通信手段と、
前記保護データの所有者を特定する情報であるトークンを生成するトークン生成手段と、
前記トークンを特定するトークン情報を生成するトークン情報生成手段と、
前記トークンを蓄積するトークン蓄積手段と、
前記保護データを特定する保護データＩＤと前記トークン情報を含む第１の情報を送信する第３の通信手段とを有する利用者装置と、
前記第１の情報を受信する第４の通信手段と、
前記保護データＩＤと等しい値を持つ前記第１の情報が既に蓄積されているかを判定する判定手段と、
前記判定手段において蓄積されていない時のみ前記第１の情報を蓄積する蓄積手段と、
既に蓄積されている前記第１の情報に対する更新情報として該第１の情報を特定する前記保護データＩＤと更新後のトークン情報とを含む第２の情報を受信する第５の通信手段と、
前記第２の情報の送信元の装置が前記第１の情報に含まれるトークン情報によって特定される前記保護データを保有していることを検証する検証手段と、
前記検証手段において保有している時のみ前記第１の情報を更新する更新手段とを有するトークン管理装置と、
前記発行者装置、前記利用者装置、前記トークン管理装置とを接続するネットワーク装置とを有することを特徴とする電子情報流通システム。
【請求項２】　前記利用者装置の前記トークン情報生成手段は、
前記トークンに対する一方向性関数の出力を利用して、前記トークン情報を生成する手段を含み、
前記トークン管理装置の前記検証手段は、
前記第２の情報の送信元から前記トークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の前記第１の情報に記録されているトークン情報に一致するかを検証する手段を含む請求項１記載の電子情報流通システム。
【請求項３】　前記トークン管理装置は、
前記蓄積手段に蓄積されている前記第１の情報に対する更新を行うために受信する前記第２の情報には、さらに、該第１の情報に含まれるトークン情報によって特定されるトークンを含み、該第２の情報の送信元の装置が、前記トークンを保有していることを判別する手段を含む請求項１または、２記載の電子情報流通システム。
【請求項４】　前記トークン管理装置は、
前記保護データＩＤを受信する手段と、
前記トークン情報蓄積手段に蓄積されている前記第１の情報の中から前記保護データＩＤが含まれる第１の情報を検索し、該第１の情報に含まれる前記トークン情報を送信する手段とを更に有し、
前記利用者装置は、
前記トークン情報を受信する手段と、
蓄積されている前記保護データＩＤによって特定される前記保護データの所有者を特定するトークンに対する一方向性関数の出力値が、前記トークン情報と一致しているかどうかを検証する手段を更に有する請求項２または、３記載の電子情報流通システム。
【請求項５】　前記トークン管理装置は、
前記第１の情報及び前記第２の情報に含まれる保護データＩＤに、前記保護データに対する一方向性関数の出力を含む請求項１、２、３、または、４記載の電子情報流通システム。
【請求項６】　前記保護データＩＤに、前記保護データのネットワーク上のアドレスを含む請求項１、２、３、４または、５記載の電子情報流通システム。
【請求項７】　電子的な情報の流通を行う電子情報流通システムにおいて、トークンを特定するトークン情報を管理するトークン管理装置に搭載される電子情報流通プログラムを格納した記憶媒体であって、
利用者装置で生成された保護データを特定する保護データＩＤとトークン情報とを含む第１の情報を受信させる第１の通信プロセスと、
前記保護データＩＤと等しい値を持つ前記第１の情報が既に蓄積されているかを判定する判定プロセスと、
前記判定プロセスにおいて蓄積されていない時のみ前記第１の情報を蓄積手段に格納する格納プロセスと、
既に前記蓄積手段に格納されている前記第１の情報に対する更新情報として該第１の情報を特定する前記保護データＩＤと更新後の新しいトークン情報とを含む第２の情報を受信する第２の通信プロセスと、
前記第２の情報の送信元の装置が前記第１の情報に含まれるトークン情報によって特定される前記トークンを保有していることを検証する検証プロセスと、前記検証プロセスにおいて保有している時のみ前記第１の情報を更新する更新プロセスとを有することを特徴とする電子情報流通プログラムを格納した記憶媒体。
【請求項８】　前記検証プロセスは、
前記第２の情報の送信元から前記トークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の前記第１の情報に記録されているトークン情報に一致するかを検証するプロセスを含む請求項７記載の電子情報流通プログラムを格納した記憶媒体。
【請求項９】　前記前記蓄積手段に蓄積されている前記第１の情報に対する更新を行うために受信する前記第２

の情報には、さらに、該第１の情報に含まれるトークン情報によって特定されるトークンを含み、該第２の情報の送信元の装置が、前記トークンを保有していることを判別するプロセスを含む請求項７または、８記載の電子情報流通プログラムを格納した記憶媒体。

【請求項１０】　前記保護データＩＤを受信する第３の通信プロセスと、

前記蓄積手段に格納されている前記第１の情報の中から前記保護データＩＤが含まれる第１の情報を検索し、該第１の情報に含まれる前記トークン情報を送信するプロセスとを更に有する請求項８または、９記載の電子情報流通プログラムを格納した記憶媒体。

【請求項１１】　電子的な情報の流通を行うための電子情報流通方法において、

多重使用を防止すべき保護データを発行する際に、

発行者装置において、保護データを生成し、利用者装置に転送し、

前記利用者装置が前記保護データを受け取ると、該保護データ毎にトークンを生成して格納しておき、該トークンと該保護データからハッシュ値で表現される保護データＩＤとトークン情報を含む発行要求を生成して、該発行者装置に転送し、

前記発行者装置は、前記発行要求に含まれている前記トークン情報と前記保護データＩＤを含むトークン情報登録要求を生成し、トークン管理装置に転送し、

前記トークン管理装置は、前記トークン情報登録要求に含まれている前記保護データＩＤが蓄積されているかを判定し、蓄積されていない場合に、該保護データＩＤに対応するのトークン情報を登録することを特徴とする電子情報流通方法。

【請求項１２】　前記保護データを譲渡する際に、

譲渡元の前記利用者装置において、譲渡対象の保護データを指定し、譲渡先の利用者装置に該保護データを転送し、

譲渡先の利用者装置は、前記保護データに対応する新たなトークンを生成して格納しておき、

前記保護データと前記新たなトークンのハッシュ値で表現されるトークン情報を含む譲渡要求を生成して、前記譲渡元の利用者装置に該譲渡要求を転送し、

前記譲渡元の利用者装置は、蓄積されている譲渡対象の保護データに対するトークンを取得し、前記譲渡要求に含まれている該保護データに対する新しいトークン情報と保護データＩＤと前記トークンとを含むトークン情報更新要求を生成し、トークン管理装置に該トークン情報更新要求を転送し、

前記トークン管理装置は、前記トークン情報更新要求に含まれている前記トークンのハッシュ値と、予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、前記保護データのトークン情報を更新する請求項１１記載の電子情報流通方法。

【請求項１３】　前記保護データを消費する際に、

前記利用者装置は、保護データ要求条件を受け取ると、その条件に合致する保護データを予め保護データが格納されている記憶手段から検索し、検索された保護データに対するトークンを取得し、改札者装置に該トークンと該保護データとを転送し、

前記改札者装置は、前記保護データのハッシュ値で表現される保護データＩＤと前記トークンを含むトークン情報削除要求を生成し、前記トークン管理装置に該削除要求を転送し、

前記トークン管理装置は、前記トークン情報削除要求に含まれている前記トークンのハッシュ値と予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、前記保護データのトークン情報を無効にする請求項１１記載の電子情報流通方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法に係り、特に、チケットやクーポン等のサービスや物を請求する権利をディジタル化した電子チケット、あるいはお金や商品券等の価値をディジタル化した電子現金のように、利用者間で転々と流通し、かつ不正な複製を防止することが必要な電子情報について、正当な電子情報の所有者を認証することを可能とする汎用的な電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法に関する。

【０００２】

【従来の技術】電子チケットや電子現金などは、一般に、複製が作られることを防止、もしくは、複製された場合に、本物と識別することが求められる。即ち、配布したデータが利用者等により複製され、それらが多重に使用されることを防ぐ必要がある。

【０００３】従来は、以下で示すような技術により、上記のような多重使用を防止しなければならないデータ（以後、保護データと呼ぶ）を流通させている。第１の方法は、保護データをＩＣカード等の耐タンパ装置に格納し、当該データを耐タンパ装置の外からは参照できないようにする。そして、当該データを利用者から利用者へ譲渡する場合には、当該耐タンパ装置間で暗号化して移動させる。譲渡者の耐タンパ装置から被譲渡者への耐タンパ装置への移動が成功した場合には、確実に譲渡者の耐タンパ装置から当該データを抹消する。これにより、各保護データが複製されないように制御する。また、保護データを使用する場合には、当該保護データを該耐タンパより抹消する。これらにより、保護データが多重譲渡あるいは多重使用されることを防止する。

【０００４】このような方式の例としては、例えば、特願平６－５０３９１３や、特表平９－５１１３５０等多

数存在し、さらに、特願平１１－３９０８０や、特願平１１－２４７４５７では、保護データ自身は通常の蓄積媒体に格納するが、当該データの原本性を示すデータ（トークン）のみを耐タンパ装置に格納することで、処理速度や記憶容量等に関して効率を向上させる方法等多数の方法が提案されている。

【０００５】第２の方法は、保護データとそのデータの所有者の識別子をセンタＤＢによって管理するものである。この方法は、保護データを利用者から利用者へ譲渡する場合に、譲渡者は、当該データに対する譲渡証明書をセンタに送り、当該データの所有者の変更を依頼する。そして、これを受け取ったセンタは、ＤＢに管理している当該データの所有者を譲渡証明書に記述された譲受者の識別子に書き換えるという方法により、各保護データに対する所有者が必ず一人になるように制御する。また、保護データを使用する場合には、使用者は、保護データに対する使用証明書をセンタに送り、当該データを使用済状態への変更を依頼する。そして、これを受け取ったセンンタは、ＤＢに管理している当該データを使用済状態に変更する。これらにより、保護データが多重譲渡あるいは、多重使用することを防止する。このような方式としては、例えば、Peter Wayner, Digital Cash, 2nd Edition, Academic Press Ltd.等に多数の方法が紹介されている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記従来の第１の方法は、システムのセキュリティが耐タンパ装置に依存し、耐タンパ装置が破られた場合の被害が大きいという問題がある。また、性能面でもシステム全体の性能が耐タンパ装置の性能に依存し、特に、耐タンパとしてＩＣカードを利用した場合には、ＩＣカードがボトルネックとなる場合が多い。さらに、ＩＣカードを使用するにあたっては、ＩＣカードリーダのような物理的な装置が必要であるが、これが利用者端末に普及していないという問題がある。

【０００７】上記従来の第２の方法は、センタで管理するため、保護データを譲渡あるいは、行使する際には、ネットワークに接続しなければならないという問題がある。この点を除いては、第１の方法に比較して、実現が比較的容易である等のメリットがある。また、ネットワークのコストが近年著しく低下してきている等の理由から、ネットワークの接続は大きなデメリットとはならなくなってきている。

【０００８】但し、第２の方法を実現する手段として、従来、譲渡証明書や使用証明書を譲渡者あるいは使用者のディジタル署名が用いられてきたが、ディジタル署名では、一般に公開鍵証明書で定義された利用者識別子によって、署名者を識別する方法がとられているが、この方法では、事前に公開鍵証明書の取得や交換を行うことが必要であり、これにより、処理効率の低下や、利用者識別子が明らかになることによるプライバシ上の問題等がある。

【０００９】また、第２の方法におけるセンタＤＢの運営は、従来、保護データの生成者であるサービス提供者自身が行うのが一般的であるが、この方法では、サービス提供者毎にセンタＤＢを運営するためコストがかかる。また、サービス提供者が勝手にセンタＤＢ上にある保護データを削除あるいは改ざんしても、利用者は手元に保護データを持たないので、その証拠を提示するのが困難である等の問題がある。

【００１０】本発明は、上記の点に鑑みなされたもので、従来の第２の方法において、公開鍵証明書の取得や、交換を必要とする公開鍵を使用せずに、ハッシュ関数のみで保護データの所有者を効率的に認証でき、かつ、内容によらず誰でも利用できる汎用的な電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】図１は、本発明の原理構成図である。本発明（請求項１）は、電子的な情報の流通を行う情報流通システムであって、電子情報であり、多重使用を防止すべき保護データを生成する保護データ生成手段３０２と、保護データを送信する第１の通信手段３０１とを有する発行者装置３００と、保護データを受信する第２の通信手段４０１と、保護データの所有者を特定する情報であるトークンを生成するトークン生成手段４０２と、トークンを特定するトークン情報を生成するトークン情報生成手段４０３と、トークンを蓄積するトークン蓄積手段４０４と、保護データを特定する保護データＩＤとトークン情報を含む第１の情報を送信する第３の通信手段４０５とを有する利用者装置４００と、第１の情報を受信する第４の通信手段２０１と、保護データＩＤと等しい値を持つ第１の情報が既に蓄積されているかを判定する判定手段２０２と、判定手段２０２において蓄積されていない時のみ第１の情報を蓄積するトークン情報蓄積手段２０３と、トークン情報蓄積手段２０３に第１の情報を登録する登録手段２０４と、既に蓄積されている第１の情報に対する更新情報として該第１の情報を特定する保護データＩＤと更新後のトークン情報とを含む第２の情報を受信する第５の通信手段２０５と、第２の情報の送信元の装置が第１の情報に含まれるトークン情報によって特定される保護データを保有していることを検証する検証手段２０６と、検証手段２０６において保有している時のみ第１の情報を更新する更新手段２０７とを有するトークン管理装置２００と、発行者装置３００、利用者装置４００、トークン管理装置２００とを接続するネットワーク装置１００とを有する。

【００１２】本発明（請求項２）は、利用者装置４００

のトークン情報生成手段４０３において、トークンに対する一方向性関数の出力を利用して、トークン情報を生成する手段を含み、トークン管理装置２００の検証手段２０６において、第２の情報の送信元からトークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の第１の情報に記録されているトークン情報に一致するかを検証する手段を含む。

【００１３】本発明（請求項３）は、トークン管理装置２００において、トークン情報蓄積手段２０３に蓄積されている第１の情報に対する更新を行うために受信する第２の情報には、さらに、該第１の情報に含まれるトークン情報によって特定されるトークンを含み、該第２の情報の送信元の装置が、トークンを保有していることを判別する手段を含む。

【００１４】本発明（請求項４）は、トークン管理装置２００において、保護データＩＤを受信する手段と、トークン情報蓄積手段２０３に蓄積されている第１の情報の中から保護データＩＤが含まれる第１の情報を検索し、該第１の情報に含まれるトークン情報を送信する手段とを更に有し、利用者装置４００において、トークン情報を受信する手段と、蓄積されている保護データＩＤによって特定される保護データの所有者を特定するトークンに対する一方向性関数の出力値が、トークン情報と一致しているかどうかを検証する手段を更に有する。

【００１５】本発明（請求項５）は、トークン管理装置２００において、第１の情報及び第２の情報に含まれる保護データＩＤに、保護データに対する一方向性関数の出力を含む。本発明（請求項６）は、保護データＩＤに、保護データのネットワーク上のアドレスを含む。

【００１６】本発明（請求項７）は、電子的な情報の流通を行う電子情報流通システムにおいて、トークンを特定するトークン情報を管理するトークン管理装置に搭載される電子情報流通プログラムを格納した記憶媒体であって、利用者装置で生成された保護データを特定する保護データＩＤとトークン情報とを含む第１の情報を受信させる第１の通信プロセスと、保護データＩＤと等しい値を持つ第１の情報が既に蓄積されているかを判定する判定プロセスと、判定プロセスにおいて蓄積されていない時のみ第１の情報を蓄積手段に格納する格納プロセスと、既に蓄積手段に格納されている第１の情報に対する更新情報として該第１の情報を特定する保護データＩＤと更新後の新しいトークン情報とを含む第２の情報を受信する第２の通信プロセスと、第２の情報の送信元の装置が第１の情報に含まれるトークン情報によって特定されるトークンを保有していることを検証する検証プロセスと、検証プロセスにおいて保有している時のみ第１の情報を更新する更新プロセスとを有する。

【００１７】本発明（請求項８）は、検証プロセスにおいて、第２の情報の送信元からトークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の第１の情報に記録されているトークン情報に一致するかを検証するプロセスを含む。本発明（請求項９）は、蓄積手段に蓄積されている第１の情報に対する更新を行うために受信する第２の情報には、さらに、該第１の情報に含まれるトークン情報によって特定されるトークンを含み、該第２の情報の送信元の装置が、トークンを保有していることを判別するプロセスを含む。

【００１８】本発明（請求項１０）は、保護データＩＤを受信する第３の通信プロセスと、蓄積手段に格納されている第１の情報の中から保護データＩＤが含まれる第１の情報を検索し、該第１の情報に含まれるトークン情報を送信するプロセスとを更に有する。本発明（請求項１１）は、電子的な情報の流通を行うための電子情報流通方法において、多重使用を防止すべき保護データを発行する際に、発行者装置において、保護データを生成し、利用者装置に転送し、利用者装置が保護データを受け取ると、該保護データ毎にトークンを生成して格納しておき、該トークンと該保護データからハッシュ値で表現される保護データＩＤとトークン情報を含む発行要求を生成して、該発行者装置に転送し、発行者装置は、発行要求に含まれているトークン情報と保護データＩＤを含むトークン情報登録要求を生成し、トークン管理装置に転送し、トークン管理装置は、トークン情報登録要求に含まれている保護データＩＤが蓄積されているかを判定し、蓄積されていない場合に、該保護データＩＤに対応するのトークン情報を登録する。

【００１９】本発明（請求項１２）は、保護データを譲渡する際に、譲渡元の利用者装置において、譲渡対象の保護データを指定し、譲渡先の利用者装置に該保護データを転送し、譲渡先の利用者装置は、保護データに対応する新たなトークンを生成して格納しておき、保護データと新たなトークンのハッシュ値で表現されるトークン情報を含む譲渡要求を生成して、譲渡元の利用者装置に該譲渡要求を転送し、譲渡元の利用者装置は、蓄積されている譲渡対象の保護データに対するトークンを取得し、譲渡要求に含まれている該保護データに対する新しいトークン情報と保護データＩＤとトークンとを含むトークン情報更新要求を生成し、トークン管理装置に該トークン情報更新要求を転送し、トークン管理装置は、トークン情報更新要求に含まれているトークン情報と、予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、保護データのトークン情報を更新する。

【００２０】本発明（請求項１３）は、保護データを消費する際に、利用者装置は、保護データ要求条件を受け取ると、その条件に合致する保護データを予め保護データが格納されている記憶手段から検索し、検索された保護データに対するトークンを取得し、改札者装置に該トークンと該保護データとを転送し、改札者装置は、保護データのハッシュ値で表現される保護データＩＤとトークンを含むトークン情報削除要求を生成し、トークン管

理装置に該削除要求を転送し、トークン管理装置は、トークン情報削除要求に含まれているトークンのハッシュ値と予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、保護データのトークン情報を無効にする。

【００２１】上記により、信頼できる第三者機関（ＴＴＰ）等が、保護データの生成者に代わって保護データの内容と、その所有者を管理することで、サービス提供者毎にセンタＤＢを運営する必要がなくなり、また、サービス提供者が勝手にセンタＤＢ上にある保護データを削除あるいは、改ざんすることを防止することが可能となる。

【００２２】

【発明の実施の形態】電子現金や電子チケットのような保護データは、一般に、発行、譲渡、使用（又は、改札）の３種類のトランザクションによって、発行者、利用者、サービス提供者の間を流通するものと見做すことができる。つまり、保護データは、発行者による発行トランザクションの実行によって生成されて利用者に渡り、利用者による譲渡トランザクションの実行により、利用者間を転々と流通し、最後に、サービス提供機関による改札トランザクション（あるいは、利用者による消費トランザクション）の実行により消滅する。

【００２３】これを実現するために、本発明では、発行者、利用者、改札者がそれぞれ保有する発行者装置、利用者装置、改札者装置と、保護データが不正にコピーされることを防止するため、保護データが本物が複製かを識別する機構であるトークン管理装置と、これらの装置を接続するネットワーク装置（インターネット等）から構成される。

【００２４】図２は、本発明の電子情報流通システムの構成を示す。同図に示す電子情報流通システムは、１つのネットワーク装置１９に接続された１個以上のトークン管理装置１１、１２、１個以上の発行装置１３、１４、１個以上の利用者装置１５、１６、１個以上の改札者装置１７、１８から構成される。

【００２５】発行装置１３、１４は、流通対象の電子情報（保護データ）を生成して転送する。利用者装置１５、１６は、発行装置で生成された保護データを受信し、当該電子情報の所有者を特定するトークン情報を生成して、蓄積する。トークン管理装置１１は、保護データを特定する保護データＩＤとトークン情報を含む管理情報（保護データＩＤ＋トークン情報）を受信し、保護データＩＤと等しい値を持つ別の情報が既に蓄積されているかを判定し、蓄積されていない時のみ、管理情報（保護データＩＤ＋トークン情報）を蓄積する。また、既に管理情報が蓄積されている更新情報として管理情報を特定する保護データＩＤと更新後の新しい所有者を特定するトークン情報とを含む更新情報（保護データＩＤ＋新トークン情報）を受信し、当該更新情報の送信元の装置が、管理情報（保護データＩＤ＋トークン情報）に含まれるトークン情報によって特定されるトークンを保有していることを検証する。検証によりトークンを保有している時のみ、管理情報（保護データＩＤ＋トークン情報）を更新情報に更新する。

【００２６】ネットワーク装置１９は、上記の各装置を接続する。

【００２７】

【実施例】以下、図面と共に本発明の実施例を説明する。

［第１の実施例］図３は、本発明の第１の実施例のトークン管理装置の構成を示す。同図に示すトークン管理装置２０は、トークン情報蓄積部２１、記録制御部部２２、公開制御部２３、及び通信部２４から構成される。各部の詳細な動作は後述する。

【００２８】図４は、本発明の第１の実施例の発行者装置の構成を示す。同図に示す発行者装置３０は、通信部３１、保護データ生成部３２、発行制御部３３から構成される。各部の詳細な動作は後述する。図５は、本発明の第１の実施例の利用者装置の構成を示す。同図に示す利用者装置４０は、通信部４１、譲渡制御部４２、譲受制御部４３、被改札制御部４４、保護情報蓄積部４５、及びトークン蓄積部４６から構成される。各部の詳細な動作は後述する。

【００２９】図６は、本発明の第１の実施例の改札者装置の構成を示す。同図に示す改札者装置５０は、通信部５１、改札制御部５２から構成される。各部の詳細な動作は後述する。上記の各装置を用いて保護データの流通を安全に行う方式を、以下（１）保護データの発行を行う発行トランザクションの場合、（２）保護データの譲渡を行う譲渡トランザクションの場合、（３）保護データの消費（改札）を行う消費（改札）トランザクションの場合に分けて説明する。なお、各装置を跨がるそれぞれの通信は、ネットワーク装置１９を介するものとする。

【００３０】（１）発行トランザクション：図７は、本発明の第１の実施例の保護データの発行を行う場合のシーケンスチャートである。

ステップ６０１）　発行者装置３０の発行制御部３３は、保護データ生成部３２により、保護データＭを生成する。保護データＭは、例えば、電子チケットの場合には、電子チケットが表象する権利の内容が記述されたディジタル情報である。但し、トークン管理装置２０が複数存在することを前提とするシステムでは、この保護データＭの中に、トークン管理装置２０の識別子が含まれているものとする。また、保護データＭの内容に対して否認防止や改ざん防止が求められる場合には、発行者による署名が施される場合もあるが、保護データＭにはこれらの署名も含まれるものとする。

【００３１】ステップ６０２）　発行者装置３０の発行

制御部３３は、通信部３１により、利用者装置４０に保護データMを転送する。

ステップ６０３）　利用者装置４０の譲受制御部４３は、通信部４１により保護データMを受け取ると、乱数K_0を生成する。このように、乱数K_0は、保護データM毎に１つ生成されるものであり、これを保護データMのトークンと呼ぶ。

【００３２】ステップ６０４）　譲受制御部４３は、保護データ蓄積部４５に保護データMを、トークン蓄積部４６にK_0を格納する。ここで、保護データは、必ずしも秘密にしておく必要がないため、保護データ蓄積部４５の内容は、利用者が管理するサーバ等で公開してもよい。一方、トークンK_0は、利用者装置４０の内部に安全に保管され、漏れないことを前提とする。

【００３３】ステップ６０５）　譲受制御部４３は、これらトークンK_0と保護データMから発行要求

$R_0 = (h(M), h(K_0))$

を生成する。ここで、h（X）は、Xのハッシュ値であり、この関数を実現する方法としては、ＲＳＡ Data Security社のＭＤ５や、米国ＮＩＳＴによって規定されたＳＨＡ等がある。

【００３４】ステップ６０６）　譲受制御部４３は、通信部４１により、生成した発行要求R_0を発行者装置３０に送る。

ステップ６０７）　発行者装置３０の発行制御部３３は、通信部３１により受け取った発行要求R_0から保護データMに対するトークンの登録要求

$IO_0 = (h(M), nil, h(K_0))$

を生成し、通信部３１によりトークン管理装置２０に登録要求IO_0を転送する。ここで、h（M）を保護データＩＤ、h（K_0）をトークン情報と呼ぶ。

【００３５】ステップ６０８）　トークン管理装置２０の記録制御部２２は、通信部２４より受け取ったトークン登録要求IO_0に含まれている保護データＩＤh（M）とトークン情報h（K_0）をトークン情報蓄積部２１に格納する。具体的には、

①　トークン情報蓄積部２１は、図８に示す構造のトークン情報管理テーブル９０を保持する。このとき、既に登録されている場合、即ち、保護データＩＤh（M）がh（m_1）…h（m_n）の何れかに一致するかどうかチェックする。

②　①の結果、もし一致するものが存在した場合には、例外を発生させ、発行トランザクションを例外終了させる。

③　①の結果、いずれにも一致しなかった場合には、保護データＩＤが保護データＩＤh（M）、トークン情報履歴が＜ｎｉｌ，h（K_0）＞という内容の行を追加する。これにより、保護データMのトークン情報は、h（K_0）と解釈することとする。つまり、K_0が保護データMのトークンとして解釈されることになる。但し、後で述べるように、トークン情報は、譲渡トランザクションによって更新される可能性がある。

【００３６】ステップ６０９）　トークン管理装置２０の記録制御部２２は、ステップ６０８が成功すると、通信部２４によりＳＵＣＣＥＳＳイベントを発行者装置３０に転送する。以上、ステップ６０１～６０９のステップの処理により、発行の基本的なフローは終了する。

【００３７】以下に示すステップ６１０～６１４は、保護データを受け取った利用者装置４０が、それが本当に自分のものであるかを検証するステップであり、省略可能である。また、これは、発行トランザクションの一部として行うこともできるし、利用者が指定した別のタイミングで行うこともできる。

ステップ６１０）　利用者装置４０の譲受制御部４３は、利用者からの指示やタイマからのイベント等を受信したことを契機に、保護データMに対するトークン情報がトークン管理装置に登録されているかを検証する要求を生成する。

【００３８】ステップ６１１）　利用者装置４０は、通信部４１により保護データMに対するトークン情報の検索要求としてh（M）を転送する。

ステップ６１２）　トークン管理装置２０の公開制御部２３は、通信部４２よりトークン情報の検索要求として、h（M）を受け取ると、トークン情報蓄積部２１に格納されているトークン情報管理テーブル９０から、保護データＩＤとしてh（M）を有する最新のトークン情報を検索する。

【００３９】ステップ６１３）　公開制御部２３は、ステップ６１２によって検索された最新のトークン情報を通信部２４によって利用者装置４に転送する。なお、ステップ６１１～ステップ６１３で行っている処理は、h（M）をキーとして、トークン情報を検索して返す単純な処理であるため、ＩＥＴＦで標準化されているＨＴＴＰプロトコルを用いて実現してもよい。

【００４０】ステップ６１４）　利用者装置４０の譲受制御部４３は、通信部４１より最新のトークン情報を受け取ると、それがトークン蓄積部４６に格納されているK_0のハッシュ値と一致するかを検証する。もし、一致すれば、自分が所有であることが確認できる。なぜなら、以上のシーケンスチャートから明らかなように、トークンK_0は、利用者装置４０自身で生成し、かつ外には出ないため、トークンK_0を知っているのは、利用者装置４０の保有者のみであるからである。

【００４１】（２）　譲渡トランザクション：以下の例では、トークン管理装置２０を介して、２つの利用者装置４０ａと４０ｂ間で保護データの譲渡を行う場合について説明する。図９は、本発明の第１の実施例の保護データ譲渡の場合の動作を示すシーケンスチャートである。

【００４２】ステップ７０１）　利用者装置４０ａの制

御部４２は、利用者に保護データ蓄積部４５に格納されている保護データの一覧を表示すること等により、譲渡対象の保護データMを指定する。

ステップ７０２）　利用者装置４０ａの譲渡制御部４２は、通信部４１により、譲渡先の利用者装置４０ｂに保護データMを転送する。

【００４３】ステップ７０３）　利用者装置４０ｂの譲受制御部４３は、通信部４１により保護データMを受け取ると、乱数K_jを生成する。この乱数K_jは、譲渡トランザクションが成功した後、保護データMの新しいトークンとなる。

ステップ７０４）　利用者装置４０ｂの譲受制御部４３は、保護データ蓄積部４５に保護データMを、トークン蓄積部４６にトークンK_jを格納する。

【００４４】ステップ７０５）　利用者装置４０ｂの譲受制御部４３は、トークンK_jと保護データMから譲渡要求

$R_j = (h(M), h(K_j))$

を生成する。ステップ７０６）　利用者装置４０ｂの譲受制御部４３は、通信部４１により、生成した譲渡要求R_jを利用者装置４０ａに送る。

【００４５】ステップ７０７）　利用者装置４０ａの譲渡制御部４２は、トークン蓄積部４６から譲渡対象の保護データMに対するトークンK_{j-1}を取得する。

ステップ７０８）　利用者装置４０ａの譲渡制御部４２は、通信部４１により受け取ったR_jとステップ７０７で獲得したトークンK_{j-1}から保護データMに対するトークンの更新要求

$IO_j = (h(M), K_{j-1}, h(K_j))$

を生成し、通信部４１によりトークン管理装置２０に更新要求IO_jを転送する。

【００４６】ステップ７０９）　トークン管理装置２０の記録制御部２２は、通信部２４より受け取った更新要求IO_jに含まれている$h(K_j)$を保護データMに対する新しいトークン情報としてトークン情報蓄積部２１に格納する。具体的には、

①　トークン情報蓄積部２１が保持するトークン情報管理テーブル９０（図８）において、$h(M) = h(m_i)$なる$h(m_i)$が存在するかどうか調べる。

②　①の結果、存在しない場合には、例外を発生させ、譲渡トランザクションを例外終了する。

③　①の結果、存在する場合には、末尾のトークン更新履歴$<k_{i,j-2}, h(k_{i,j-1})>$　（$j>1$，$j=1$のとき、$k_{i,j-2}=nil$）中の$h(k_{i,j-1})$と、受け取った更新要求IO_jのトークンK_{j-1}から計算した$h(K_{j-1})$の値が等しいかチェックする。

④　③の結果、等しくない場合には、例外を発生させ、譲渡トランザクションを例外終了させる。

⑤　③の結果、等しい場合には、新たな更新履歴として、$<K_{j-1}, h(K_j)>$を追加する。これにより、保護データMのトークン情報は$h(K_j)$に更新されたと解釈する。つまり、K_jがMの唯一のトークンとして解釈されることになる。

【００４７】ステップ７１０）　トークン管理装置２０の記録制御部２２は、ステップ７０９が成功すると、通信部２４によりＳＵＣＣＥＳＳイベントを利用者装置４０ａに転送する。以上、ステップ７０１～７１０のステップの処理により、譲渡の基本的なフローは終了する。

【００４８】以下に示すステップ７１１～７１５は、保護データを受け取った利用者装置４０ｂが、それが本当に自分のものであるかを検証するステップであり、省略可能である。また、これは、譲渡トランザクションの一部として行うこともできるし、利用者が指定した別のタイミングで行うこともできる。

ステップ７１１）　利用者装置４０ｂの譲受制御部４３は、利用者からの指示やタイマからのイベント等を受信したことを契機に、保護データMに対する新しいトークン情報がトークン管理装置２０に登録されているかを検証する要求を生成する。

【００４９】ステップ７１２）　利用者装置４０ｂは、通信部４１により保護データMに対するトークン情報の検索要求として$h(M)$を転送する。

ステップ７１３）　トークン管理装置２０の公開制御部２３は、通信部２４より、トークン情報の検索要求として$h(M)$を受け取ると、トークン情報蓄積部２１に格納されているトークン情報管理テーブル９０（図８）から保護データＩＤとして$h(M)$を有する最新のトークン情報を検索する。

【００５０】ステップ７１４）　公開制御部２３は、ステップ７１２によって検索された最新のトークン情報を通信部２４によって利用者装置４０に転送する。なお、ステップ７１２～ステップ７１４で行っている処理は、$h(M)$をキーとしてトークン情報を検索して返す単純な処理であるため、ＩＥＴＦで標準化されているＨＴＴＰプロトコルを用いて実現してもよい。

【００５１】ステップ７１５）　利用者装置４０ｂの譲受制御部４３は、通信部４１より最新のトークン情報を受け取ると、当該トークン情報がトークン蓄積部４６に格納されているK_jのハッシュ値と一致するかを検証する。もし、一致すれば、自分が所有者であることが確認できる。なぜなら、以上のシーケンスチャートから明らかなように、K_jは、利用者装置４０ｂ自身で生成し、かつ外には出ないため、K_jを知っているのは、利用者装置４０ｂの保有者のみであるからである。

【００５２】ある保護データM（$=m_i$）が、以上で述べたシーケンスチャートにより、発行者装置３０により発行され、ｊ個の利用者装置４０間で譲渡が行われたとすると、図８に示すような

$<nil, h(k_{i,0})>, <k_{i,0}, h(k_{i,1})>, \cdots, <k_{i,j-1}, h(k_{i,j})>$

というトークン情報更新履歴が作られる。この結果、流通過程で生成されたトークン$k_{i,0}$，…、$k_{i,j-1}$は、公開され、無効なものとなり、唯一$k_{i,j}$のみが公開されない。このため、$k_{i,j}$を知っている最後に譲渡された者のみが有効な所有者とすることができる。

【００５３】（３） 消費（改札）トランザクション：図１０は、本発明の第１の実施例の保護データ更新の場合の動作を示すシーケンスチャートである。

ステップ８０１） 改札者装置５０の改札制御部５２は、通信部５１により、改札対象の利用者装置４０に保護データ要求条件を転送する。保護データ要求条件の指定方法の詳細は述べないが、改札対象の保護データに含まれる属性値などに関する条件を指定する。

【００５４】ステップ８０２） 利用者装置４０の被改札制御部４４は、通信部４１により、保護データ要求条件を受け取ると、その条件に合致する保護データMを保護データ蓄積部４５から検索し、取得する。

ステップ８０３） ステップ８０２によって取得した保護データMに対するトークンK_jを取得する。

【００５５】ステップ８０４） 利用者装置４０の被改札制御部４４は、通信部４１により、改札者装置５０に保護データM及びトークンK_jを転送する。

ステップ８０５） 改札者装置５０の改札制御部５２は、通信部５１により受け取った保護データM及びトークンK_jから保護データMに対するトークンの削除要求IO_{j+1}＝（h（M），K_j，ｎｉｌ）を生成し、通信部５１によりトークン管理装置２０に当該削除要求IO_{j+1}を転送する。

【００５６】ステップ８０６） トークン管理装置２０の記録制御部２２は、通信部２４より受け取った削除要求IO_{j+1}のh（M）によって指定されるトークン情報を無効にする。具体的には、

① トークン情報蓄積部２１が保持するトークン情報管理テーブル９０（図8）において、h（M）＝h（m_i）なるh（m_i）が存在するかどうか調べる。

② ①の結果、存在しない場合には、例外を発生し、改札トランザクションを例外終了する。

③ ①の結果、存在する場合には、末尾のトークン更新履歴＜$k_{i,j-1}$，h（$k_{i,j}$）＞中のh（$k_{i,j}$）と、受け取ったIO_{j+1}中のK_jから計算したh（K_j）の値が等しいかチェックする。

④ ③の結果、等しくない場合には、例外を発生させ、譲渡トランザクションを例外終了させる。

⑤ ③の結果、等しい場合には、新たな更新履歴として、＜K_j，ｎｉｌ＞を追加する。これにより、保護データMのトークン情報は、ｎｉｌに更新されたと解釈する。つまり、保護データMのトークンは存在しないものと解釈されることになる。

【００５７】ステップ８０７） トークン管理装置２０の記録制御部２２は、ステップ８０６が成功すると、通信部２４により、ＳＵＣＣＥＳＳイベントを改札者装置５０に転送する。

ステップ８０８） 改札者装置５０の改札制御部５２は、利用者装置４０あるいは、利用者に対して、保護データMを改札した引換えとして、サービスや物を提供する（保護データがチケットの場合）。

【００５８】上記で示したシーケンスチャートによる実施例は本発明における一例であり、本発明の別の実施例として以下に示すような例も可能である。

［第２の実施例］前述の第１の実施例の図７に示す発行トランザクションにおけるステップ６０６とステップ６０７をマージして、利用者装置４０からトークン管理装置２０に対して直接トークンの登録要求IO_0を送付してもよい。

【００５９】同様に、図９における譲渡トランザクションにおけるステップ７０７をステップ７０２の前に行い、ステップ７０２において、予め利用者装置４０ａから利用者装置４０ｂに保護データMと一緒にトークンK_0を転送しておくことにより、ステップ７０６とステップ７０８をマージして利用者装置４０ｂから利用者装置４０ａに対して、直接トークンの登録要求IO_jを送付してもよい。

【００６０】同様に、図１０における消費（行使）トランザクションにおけるステップ８０４とステップ８０５をマージして、利用者装置４０から改札者装置５０に対して直接IO_{j+1}を送付してもよい。

［第３の実施例］トークン管理装置２０におけるトークン情報蓄積部２１に記録されるトークン情報の管理テーブル９０の構造は一例であり、例えば、図１１に示すように、トークン情報の変更履歴を全て保管するのではなく、各保護データm_iに対するその時点で有効なトークン情報h（$k_{i,j}$）のみを保管するようにしてもよい。

【００６１】この場合でも、上記の実施例と同様に、このトークン情報を更新あるいは無効かできるのは、$k_{i,j}$を持っている利用者装置４０だけである。

［第４の実施例］トークン管理装置２０に、課金機能を付与し、トークン情報登録要求、あるいは、トークン情報更新要求、あるいは、トークン情報無効化要求毎に、利用料を徴収することも可能である。

【００６２】課金機能の実現方法については、詳細は述べないが、例えば、トークン管理装置２０の利用を会員制とし、トークン管理装置２０の利用に先立ち特定の会員証（ディジタル証明書）等による認証を行い、利用履歴を記録し、クレジットカードや銀行振込により、利用者頻度に応じて使用料を徴収する方法、compaq社のMillicent やRivestらのPayword 等のマイクロペイメント方法等様々な方法が考えられる。

【００６３】また、トークン情報には、有効期限を付与し、有効期限内でのみ、トークン情報の公開を行うこともできる。有効期限の付与は、トークン管理装置２０毎

に与える方法、保護データ単位に与える方法、トークン情報単位に与える方法等がある。特に、トークン情報を単に与えた場合には、利用者装置４０は、自分自身の利用者装置４０に譲渡することで、トークンを更新することにより、有効期限を延長することもできる。この機能と課金処理を組み合わせることにより、利用時間に応じて料金を徴収するシステムをトークン管理装置によって代行することも可能となる。

【００６４】また、上記の実施例では、図７～図１０のシーケンスチャートに基づいて説明しているが、この例に限定されることなく、各シーケンスチャートにおける装置毎にその動作をプログラムとして構築し、本発明を実施する際に、発行者装置３０、利用者装置４０、トークン管理装置２０及び改札装置５０として利用されるコンピュータに接続されるディスク装置や、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現することが可能である。

【００６５】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において種々変更・応用が可能である。

【００６６】

【発明の効果】上述のように、本発明によれば、保護データの内容に依存せずに、保護データ毎に存在するトークンをただ一つに限定することができるので、トークンを保持しているかどうかで保護データの正当な所有者かどうかを識別することができる。これにより、保護データが不正に複数の利用者に転送されても、更には、たとえ、公開情報となっても、保護データの正規の所有者かどうかを判定することができる。しかも、保護データに対する正当なトークンを所有している者は、自分がその保護データの唯一の所有者であることを、誰にも（トークン管理装置にさえ）知られることなく、確認することができる。

【００６７】また、トークン自体の管理は、利用者あるいは、利用者装置に任されているので、ＩＣカード等の耐タンパ装置だけではなく、利用者の責任でハードディスク等に自由に複製をとることも可能である。それでも、保護データが譲渡あるいは、消費された場合には、その利用者が保持しているすべてのトークンは無効化されるので、二重譲渡や、二重使用は防止することができる。

【００６８】また、トークン管理装置を利用するにあたっては、本発明の利用者装置を保持するだけでよく、特定の機関から発行されたディジタル証明書等を事前に取得しておく必要はない。また、保護データの所有者かどうかは使い捨ての乱数で生成したトークンが使われるので、匿名性を保証できる。

【００６９】さらに、アルゴリズムとしては、計算量を必要とする公開鍵方式を必須とせず、ハッシュ関数のみで実現できるため、極めて高速に処理を行うことができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の電子情報流通システムの構成図である。

【図３】本発明の第１の実施例のトークン管理装置の構成図である。

【図４】本発明の第１の実施例の発行者装置の構成図である。

【図５】本発明の第１の実施例の利用者装置の構成図である。

【図６】本発明の第１の実施例の改札者装置の構成図である。

【図７】本発明の第１の実施例の保護データ発行の場合の動作を示すシーケンスチャートである。

【図８】本発明の第１の実施例のトークン情報の管理テーブルである。

【図９】本発明の第１の実施例の保護データ譲渡の場合の動作を示すシーケンスチャートである。

【図１０】本発明の第１の実施例の保護データ行使の場合の動作を示すシーケンスチャートである。

【図１１】本発明の第３の実施例のトークン情報の管理テーブルの例である。

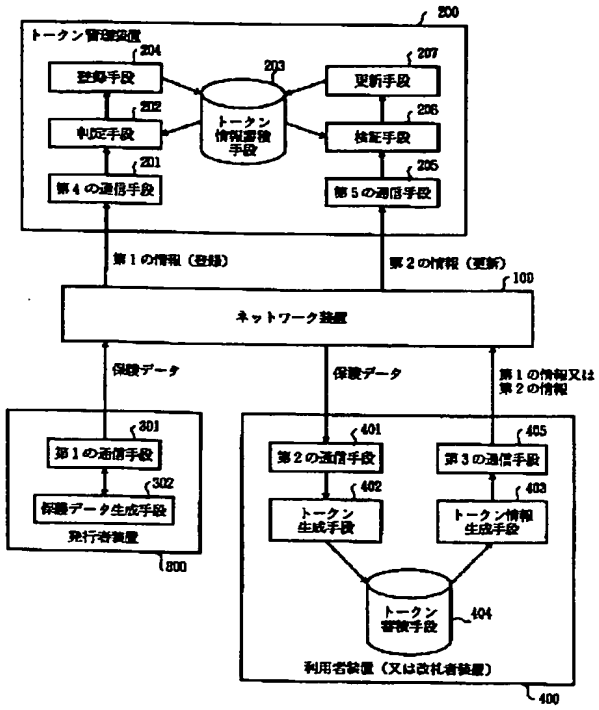
【符号の説明】

１１，１２，２０，２００　トークン管理装置
１３，１４，３０，３００　発行者装置
１５，１６，４０，４００　利用者装置
１７，１８，５０　改札者装置
１９，１００　ネットワーク装置
２１　トークン情報蓄積部
２２　記録制御部
２３　公開制御部
２４　通信部
３１　通信部
３２　保護データ生成部
３３　発行制御部
４１　通信部
４２　譲渡制御部
４３　譲受制御部
４４　被改札制御部
４５　保護データ蓄積部
４６　トークン蓄積部
５１　通信部
５２　改札制御部
１００　ネットワーク装置
２００　トークン管理装置
２０１　第４の通信手段
２０２　判定手段

２０３　トークン情報蓄積手段
２０４　登録手段
２０５　第５の通信手段
２０６　検証手段
２０７　更新手段
３００　発行者装置
３０１　第１の通信手段
３０２　保護データ生成手段
４００　利用者装置（または、改札者装置）
４０１　第２の通信手段
４０２　トークン生成手段
４０３　トークン情報生成手段
４０４　トークン蓄積手段
４０５　第３の通信手段

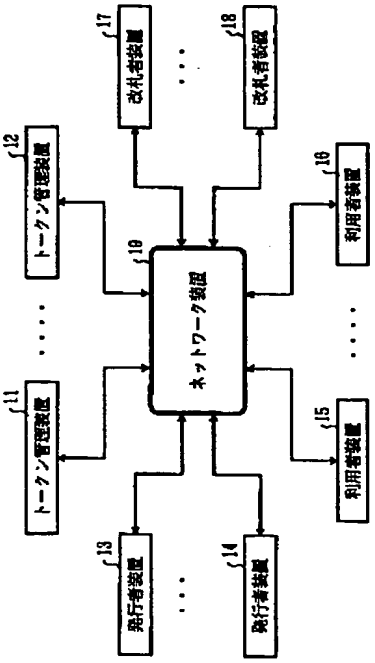
【図１】

本発明の原理構成図



【図２】

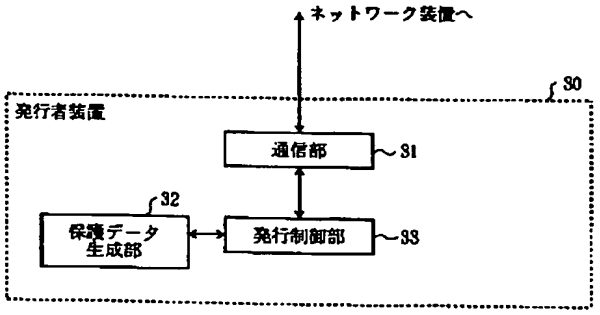
本発明の電子情報流通システムの構成図



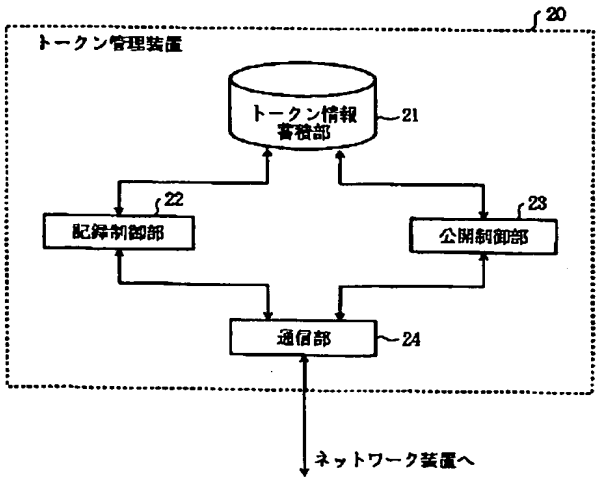
【図３】

【図４】

本発明の第１の実施例の発行者装置の構成図

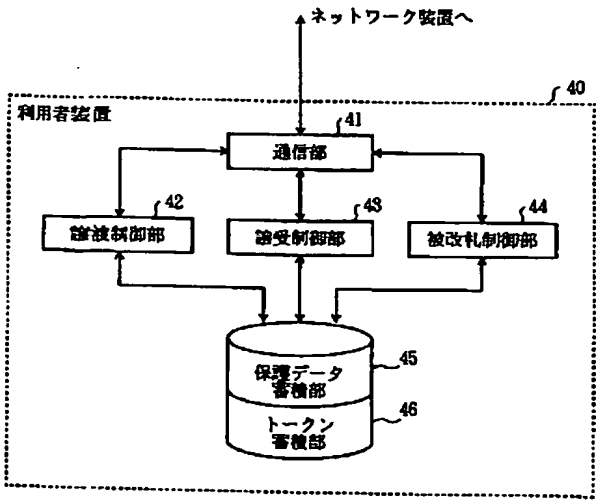


本発明の第１実施例のトークン管理装置の構成図



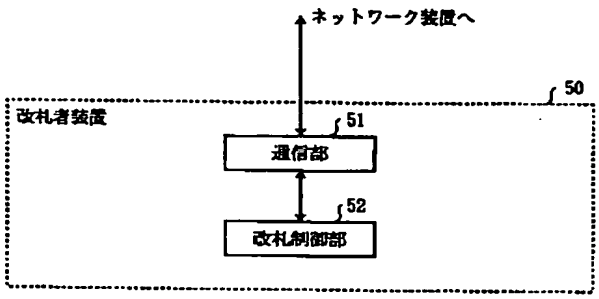
【図５】

本発明の第１の実施例の利用者装置の構成図



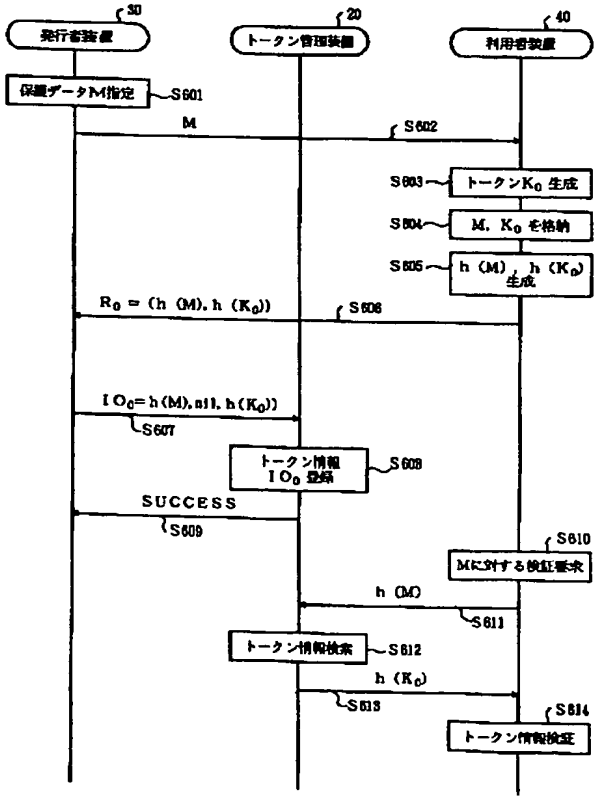
【図６】

本発明の第１の実施例の改札者装置の構成図



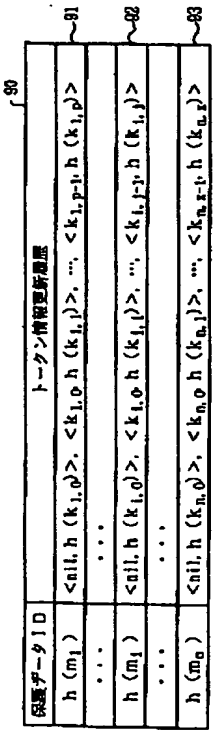
【図７】

本発明の第１の実施例の保護データ発行の場合の動作を示すシーケンスチャート



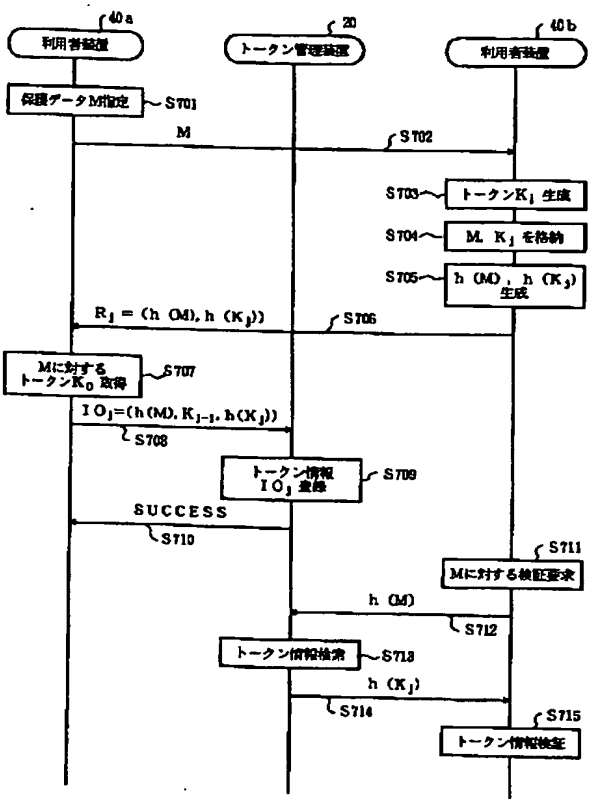
【図８】

本発明の第１の実施例のトークン情報の管理テーブル



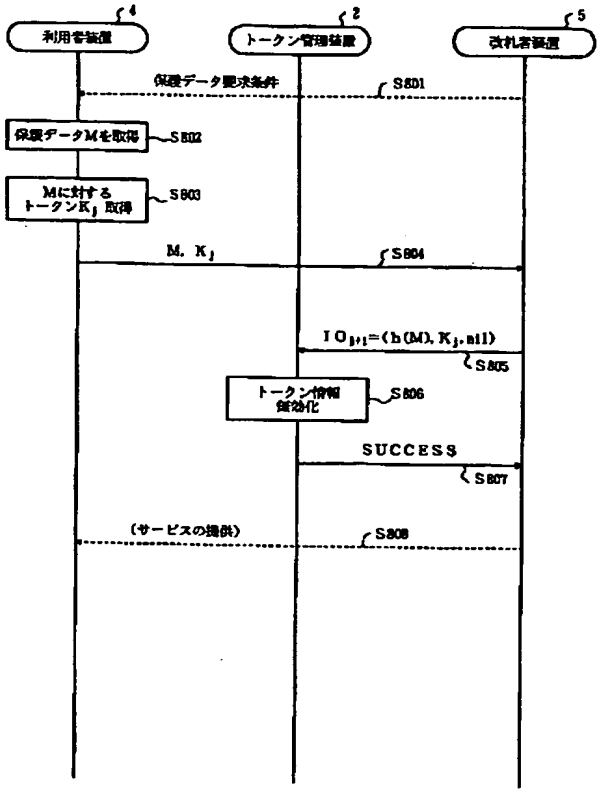
【図９】

本発明の第１の実施例の保護データ譲渡の場合の動作を示すシーケンスチャート



【図１０】

本発明の第１の実施例の保護データ行使の場合の動作を示すシーケンスチャート



【図１１】

本発明の第３の実施例のトークン情報の管理テーブル（別の実施例）

100

保護データID	トークン情報	
h (m_1)	h ($k_{1,j}$)	101
・・・	・・・	
h (m_i)	h ($k_{i,j}$)	102
・・・	・・・	
h (m_n)	h ($k_{n,x}$)	103

フロントページの続き

(51) Int. Cl.[7]	識別記号	FI		テーマコード（参考）
		G06F	15/30	360
			15/40	310F
				310C
				370Z

15/411 310

(72)発明者 寺田 雅之
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内

Ｆターム(参考) 5B049 AA05 BB11 BB46 BB61 CC05 CC16 CC39 DD04 DD05 EE03 EE05 EE23 FF09 GG04 GG07 GG10
5B055 BB10 CB09 CB10 EE02 EE03 EE17 EE21 EE27 FA05 FB03 HA12 JJ05 KK01 KK09
5B075 KK03 KK07 KK13 KK33 ND03 ND20 ND23 NK10 NK13 NK24 NK45 NK54 PP30 PQ05 PR03 UU40
5J104 AA07 KA01 NA12 PA07 PA12